CLAIMS

We claim

1. An apparatus for secure distribution of content comprising:

(a) a source for accessing content data;

(b) a conditional access module for receiving the content data from said source and selectively processing the content data and selectively authorizing access to decoded processed content data;

(c) a receiver for receiving the processed content data from said conditional access module and decoding the processed content data into said decoded processed content data; and

(d) an output device for receiving the decoded processed content data from said receiver and outputting the decoded processed content data when authorized by said conditional access module.

2. The apparatus according to claim 1 wherein said source comprises an optical disc reader.

3. The apparatus according to claim 2 wherein said optical disc reader is a DVD optical disc reader.

4. The apparatus according to claim 1, wherein the apparatus is used with a backend system and wherein said source further comprises:

(a) a source modem for communicating with said receiver and said backend; and

(b) a modem switch for switching between any two devices within the group consisting of said receiver, said source modem, and said backend.

5. The apparatus according to claim 1, wherein the apparatus is used with a backend system and wherein said receiver further comprises a receiver modem for communicating with said conditional access module, said source, and said backend.

6. The apparatus according to claim 1, wherein said content data is encrypted and said conditional access module further comprises a content decrypter to decrypt said encrypted content data into the processed content.

7. The apparatus according to claim 6, wherein said source further comprises a super encryption device for super encrypting the encrypted content data and wherein said conditional access module further comprises a super decryption device for super decrypting the super encrypted content data.

8. The apparatus according to claim 1, wherein said conditional access module further comprises an interface encryption device for encrypting the processed content data and wherein said receiver further comprises an interface decryption device for decrypting the interface encrypted processed content data.

9. The apparatus according to claim 1, wherein said conditional access module is renewable.

10. The apparatus according to claim 1, wherein said conditional access module further includes a CAM fingerprint logic device for adding a CAM watermark to said content data.

11. The apparatus according to claim 10, wherein said CAM watermark includes at least one of the following:

(a) a time of access of said content data;

(b) a serial number of said content data;

(c) a source identification value;

(d) a receiver identification value; and

(e) a conditional access module identification value.

12. The apparatus according to claim 1, further comprising a copy protection and playback control device for:

(a) receiving extracted watermark data from said output device;

(b) determining whether said extracted watermark data authorizes output of said decoded processed content data; and

(c) if so, outputting an authorization to the output device.

13. The apparatus according to claim 1, wherein said output device further includes a display device and a watermark logic device, wherein said watermark logic device is operable to:

(a) extract a watermark from said decoded processed content data;

(b) create an extracted watermark data packet from said watermark;

(c) output said extracted watermark data packet to said conditional access module;

(d) input an authorization from said conditional access module; and

(e) output an enable signal to said display device.

14. The apparatus according to claim 1, wherein said output device further includes:

(a) a video logic device for converting said decoded processed content data into a content signal; and

(b) a display device for converting said content signal into a visual and/or audible form.

15. The apparatus according to claim 14, wherein said output device further includes an output fingerprint logic device for adding an output watermark to said content signal.

16. The apparatus according to claim 15, wherein said output watermark includes at least one of the following:

(a) a time of access of said content data;

(b) a serial number of said content data;

(c) a source identification value;

(d) a receiver identification value;

(e) a conditional access module identification value; and

(f) a monitor identification value.

17. The apparatus according to claim 4, wherein said backend further includes a certifying and registering means for certifying and registering with the backend at least one device of the group consisting of: said source, said receiver, said conditional access module, and said output device.

18. An apparatus for secure distribution of content comprising:

(a) a source for accessing content data, said source including a transport packet generation device for transforming the content data into content data packets;

(b) a conditional access module for receiving the content data packets from said source and selectively processing the content data packets;

(c) a receiver for receiving the processed content data packets from said conditional access module and decoding the processed content data packets; and

(d) an output device for outputting the decoded content data,

wherein communications between the source, the receiver and the conditional access module utilize at least one packet data protocol.

19. A method of preventing unauthorized access to content data in a system comprising a source, a conditional access module, a receiver and an output device, the method comprising:

(a) acquiring content data at said source;

(b) transporting said content data to said conditional access module;

(c) determining whether access to said content data is authorized;

(d) selectively processing the content data;

(e) transporting processed content data from the conditional access module to said receiver;

(f) decoding the processed content data;

(g) selectively providing said decoded processed content data to said output device; and

(h) outputting the decoded processed content data when authorized by said conditional access module.

20. The method according to claim 19, wherein the system is used with a backend, said method further comprising the step of registering and certifying with the backend at least one device of the group consisting of: said source, said receiver, said conditional access module, and said output device.

21. The method according to claim 19, wherein said source further comprises a transport packet generating device and said step of transporting said content data to said conditional access module further comprises the step of transforming the content data into content data packets using said transport packet generating device.

22. The method according to claim 21, wherein said receiver further comprises a transport packet demultiplexer and said step of transporting said content data to said conditional access module further comprises the step of unpacking said content data packets.

23. The method according to claim 19, the method further comprising the step of adding a CAM watermark to said content data, said CAM watermark including at least one of the following:

(a) a time of access of said content data;

(b) a serial number of said content data;

(c) a source identification value;

(d) a receiver identification value; and

(e) a conditional access module identification value.

24. The method according to claim 19, wherein said system further comprises a copy protection and playback control device and wherein said step of determining whether access to said content data is authorized further comprises the steps of:

(a) transporting extracted watermark data from said output device to said copy protection and playback control device;

(b) determining whether said extracted watermark data authorizes said decoded processed content data for output; and

(c) if so, outputting an authorization to the output device.

25. The method according to claim 19, wherein said output device further includes a display device and a watermark logic device and said step of outputting the decoded processed content data when authorized by said conditional access module further comprises the steps of:

(a) extracting a watermark from said decoded processed content data;

(b) determining whether said watermark is different from a predetermined watermark or if a predetermined amount of time has expired;

(c) if the watermark is determined to be different or said predetermined amount of time has expired:

(i) outputting said extracted watermark data to said conditional access module;

(ii) receiving an authorization from said conditional access module; and

(iii) outputting an enable signal to said display device if authorized.

26. The method according to claim 19, wherein said step of outputting the decoded processed content data further includes:

(a) converting said decoded processed content data into a content signal; and

(b) converting said content signal into a visual and/or audible form.

27. The method according to claim 26, the method further comprising the step of adding an output watermark to said content signal, said output watermark including at least one of the following:

(a) a time of access of said content data;

(b) a serial number of said content data;

(c) a source identification value;

(d) a receiver identification value;

(e) a conditional access module identification value; and

(f) a monitor device identification value.

28. The method according to claim 19, wherein said content data is encrypted and said step of selectively processing the content data further comprises the step of decrypting said encrypted content data.

29. The method according to claim 19, wherein said step of said transporting said content data to said conditional access module further comprises the steps of:

(i) super encrypting said content data;

(ii) transporting said content data to said conditional access module; and

(iii) super decrypting the super encrypted content data.

30. The method according to claim 19, wherein said step of said transporting processed content data from the conditional access module to said receiver further comprises the steps of:

(i) encrypting said processed content data;

(ii) transporting encrypted processed content data to said receiver; and

(iii) decrypting the decrypted processed content data.

31. A method of preventing unauthorized access to content data in a system comprising a source, a conditional access module, a receiver and an output device, the method comprising:

a) acquiring content data at said source;

b) transforming said content data into packet data;

c) transporting said packet data from said source to said conditional access module;

d) determining whether access to said packet data is authorized;

e) selectively process said packet data;

f) transporting said processed packet data to said receiver;

g) decoding said processed packet data; and

h) outputting the decoded content.

wherein communications between the source, the receiver and the conditional access module utilize at least one packet data protocol.